A

Synopsis

On

A Study of Rank Metric Codes and Subspace Codes

Submitted to

Swami Ramanand Teerth Marathwada University
Nanded-431606, Maharashtra State, India

For the Degree of

Doctor of Philosophy(Ph.D.)

In Mathematics(Faculty of Sciences and Technology)

Submitted by

Miss. Patil Bhagyashri S.

Research Student

Under the Guidance of

Dr. Jogdand Suryakant M.

Professor and Head
Department of Mathematics,
SSGM College Loha,
SRTM University, Nanded-431606.

March 2022

1 Introduction

Coding theory deals with the design of error-correcting codes for the reliable transmission of information across noisy channels. Error-correcting codes are clever ways of representing data so that one can recover the original information even if parts of it are corrupted. The main objects of coding theory are vector spaces with a metric. Error-correcting codes are based on the Hamming metric:the codewords are vectors and the distance between two codewords is their Hamming distance. In some circumstances, we may want to use different kinds of codewords and a different metric. For error detection and correction of codes the minimum Hamming distance (it will be called minimum distance and denoted by d hereafter) plays very important role. If d is distance of code then the code can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors. Thus larger the minimum Hamming distance maximum the error capability. But we have the limitations of maximum value of d which is given by a well known Singleton bound $d \leq n - k + 1$. Therefore for good codes in terms of maximum distance recently researchers are trying to construct codes from algebraic curves, from different sub spaces of vector spaces, space of matrices of any order by concatenation of available codes. Some of such codes are Subspace codes, Rank metric codes, Quasi-cyclic, Negacyclic codes. Rank metric codes has two representations as matrix representation and vector representation. Subspace codes and Rank Metric Codes can be used to correct errors in network coding. The Rank Metric Codes were first introduced by Delsarte in [1] and Subspace Codes were introduced by Koetter and Kschischang.

In the proposed Ph. D. thesis work I would like to study Rank Metric Codes and Subspace Codes and their concatenations in various ways. The weight distribution properties of these codes is also the subject of my interest during my research.

2 Review of Literature and Development in The Subject

Coding theory became the subject of mathematical interest due to the landmark paper, *A Mathematical Theory of Communication* by Shannon [9] in the year 1949 who gave the explicit definition of information. This paper is popularly recognized as the magna Carta of information

age. In subsequent years Richard Hamming [8] contributed immensely in this area. In coding theory an electronic information could be transmitted through a noisy channel where an error is likely to happen. Usually the message is sent in a string of binary digits 0's and 1's which are the elements of binary field $\mathbb{F}_2 = \{0, 1\}$. But, for algebraic and combinatorial interest $\mathbb{F}_2$ can be replaced by any finite field $\mathbb{F}_q$ (where q power of any prime) or by any finite ring R. These alphabets have a great algebraic structure and their structures leads to construct various useful codes. This is also one of the reasons that the algebraic coding theory has become a separate subject of interests to many mathematicians. It has various connections to combinatorics, graph theory, lattice theory, algebraic geometry, topology, etc.

Let q be a power of some prime p and let $\mathbb{F}_q$ denote the finite field with q elements. Let m, n be positive integers. Let $\mathbb{F}_q^{n\times m}$ denote the $\mathbb{F}_q$ -vector space of matrices of size $n \times m$ with entries in $\mathbb{F}_q$.

Let $P_q(n)$ denote the set of all subspaces of $\mathbb{F}_q^n$ which is is called the projective space of order n over $\mathbb{F}_q$. For an integer ℓ, $0 \leq \ell \leq m$, let $G(\ell, m)$ denote the set of all ℓ-dimensional subspaces of $\mathbb{F}_q^m$ and is called the Grassmanian. A subspace code is a nonempty subset of $P_q(n)$. A Grassmannian code is a nonempty subset of $G(\ell, m)$ which is also called a constant dimension code, that is, the codewords in$G(\ell, m)$ are sub spaces of $\mathbb{F}_q^m$ of dimension ℓ. Subspace codes have practical importance in network coding [2]. There are two representations of rank codes: matrix representation and vector representation. In matrix representation, rank codes are defined as subsets of a normed space $\left\{\mathbb{F}_q^{N\times n}, Rk\right\}\big)$ of $N \times n$ matrices over a finite (base) field $\mathbb{F}_q$, where the norm of a matrix $M \in \mathbb{F}_q^{N\times n}$ is defined to be the algebraic rank $Rk(M)$ of this matrix over $\mathbb{F}_q$. The rank distance between two matrices M_1 and M_2 is the rank of their difference $Rk(M_1-M_2)$. The rank distance of a matrix rank code $M \subset \mathbb{F}_q^{N\times n}$ is defined as the minimal pairwise distance: $d(M) = d = min(Rk(Mi - Mj) : Mi, Mj \in M, i \neq j)$. In vector representation, rank codes are defined as subsets of a normed n-dimensional space of $\left\{\mathbb{F}_q^{N\times n}, Rk\right\}\big)$ of n-vectors over an extension field $\mathbb{F}_{q^n}$, where the norm of a vector $v \in \mathbb{F}_q$ is defined to be the column rank $Rk(\mathrm{v} \mid \mathbb{F}_q)$ of this vector over $\mathbb{F}_q$, i.e., the maximal number of co-ordinates of v which are linearly independent over the base field $\mathbb{F}_q$. The rank distance between two vectors M_1 and M_2 is the rank of their difference $Rk(M_1-M_2)$. The rank distance of a matrix rank code $M \subset \mathbb{F}_q^{N\times n}$

is defined as the minimal pairwise distance: $d(V) = d = min(Rk(v_1 - v_2) : v_i, v_j \in V, i \neq j)$ [6]

3 Aim and Objective of Research

The main objective of my research during Ph.D. is to work on certain problems associated to Rank Metric codes and Subspace codes over finite fields, finite rings:

(i) We will investigate and expand some properties of Rank Metric codes.

(ii) We will study weight distribution of Rank Metric , Subspace, Cyclic, Constacyclic, Negacyclic codes and their duals over finite fields and finite rings.

(iii) We will study concatanation of some available codes over finite fileds and finte rings and their extensions.

(iv) We will explore the algebraic geometric codes and open problems in this area of research.

4 Methodology to be Adopted

My area of research is theoretical in nature. Mostly, I will be referring the text books and research papers of various researchers who have developed this area of research. I would also like to consult with my thesis supervisor time to time to discuss the doubts. I would also like to participate in the schools, seminars, workshops in my area of research, which will help me to strengthen my knowledge in my field of research.

5 Importance of Study

The area of my research is highly applicable in coding theory. Coding theory has its origins in the engineering problem of effective electronic communication where the alphabet is generally the binary field. Since its inception, it has grown as a branch of mathematics, and has since been expanded to consider any finite fields, and later also finite rings, as its alphabet. This proposal will presents a broad view of the subject and relates major results by ring theory.

6 Proposed Work Plan

Following is the Year-wise plan of work and target to be achieved during my research period:

Year 1:

Course work and reading : I will complete the course work and other academic formalities declared by SRTMU Nanded in the first semester. Then after, I would like to read the following text books to develop necessary background for my research:

(i) R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, rev. ed. Cambridge, England: Cambridge University Press, (1994).

(ii) F. J. MacWilliams and N. J. A. Sloane, *The Theorey of Error Correcting Codes*, North Holland, Amsterdam, 1977.

(iii) Ling, S., & Xing, C.,*Coding theory: a first course*, Cambridge University Press,Chicago,2004

Year 2:

I would like to read the research papers, text books, and would like to complete research related literature survey and decide the problem for my PhD thesis in consultation with my thesis supervisor. I would also like to participate in various national and international workshops, schools and conferences to get the broader view and to develop academic relations with other reserachers who are working in my field.

Year 3: I will focus on my research problem and would like to learn various techniques and methods by the other researchers on my area of research.

Year 4: I will try to solve my thesis problem and try to have my publications related to my work.

Year 5: I will try to write my thesis and submit to university for the award of PhD.

References

[1] I. Blak, Codes over certain rings. Inf. control, 29(4), 295-300 (1975).

[2] Hernandez, B. S., Sison, V. P.,Rank-metric codes as ideals for subspace codes and their weight properties,AKCE International Journal of Graphs and Combinatorics, 16(2), 190-197,(2019).

[3] Koetter, R., & Kschischang, F. R. (2008). Coding for errors and erasures in random network coding. IEEE Transactions on Information theory, 54(8), 3579-3591.

[4] De La Cruz, J., Gorla, E., Lopez, H. H., & Ravagnani, A. (2015). Rank distribution of Delsarte codes. arXiv preprint arXiv:1510.01008.

[5] Tsfasman, M. A., & Vladut, S. G. (1995). Geometric approach to higher weights. IEEE Transactions on Information Theory, 41(6), 1564-1588.

[6] Gabidulin, E. M.,Rank-metric codes and applications,Moscow Inst. Phys. Technol., State Univ., Dolgoprudny, Russia.

[7] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, rev. ed. Cambridge, England: Cambridge University Press, (1994).

[8] R. Hamming, Error detecting and error correcting codes. Bell Syst. Tech. J. 29, 147-160 (1950).

[9] C. Shannon, A mathematical theory of communication. Bell Syst. Techn. J. 27 (1948).

[10] M. Shi, A. Alahmadi, and P. Sole,Codes and Rings: Theory and Practice, Academic Press (2017).

[11] K. Guenda, New MDS self-dual codes over finite fields, Des. Codes Cryptogr., 62, 31-42 (2012).

[12] B. Yildiz and S. Karadeniz, Cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, Des. Codes Cryptogr., 58, 221-234 (2011).

[13] S. Zhu and L. Wang, A class of constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ and its Gray image, Discrete Mathematics, 311, 2677-2682 (2011).

[14] T. Abualrub and I. Siap, Constacyclic codes over F2 + uF2, J. Franklin Inst., 346, 520–529, 2009

[15] C. T. Ryan, *Projective codes based on Grassmann varieties* , Congr. Numer. 57, 273-279, 1987

[16] F. J. MacWilliams and N. J. A. Sloane, *The Theorey of Error Correcting Codes*, North Holland, Amsterdam, 1977.

Miss. Patil Bhagyashri Sangameshwar
Research Student

Dr. Suryakant M. Jogdand
Research Guide